Ein Verlagsbeihefter der Heise Zeitschriften Verlag GmbH & Co. KG



extra Security

Veranstaltungen

26. – 28. Februar, Nürnberg
Embedded World
www.embedded-world.de

27. – 28. Februar, Mörfelden
Web Security Days – Safety first!
www.websecdays.de

4. – 9. März, Hannover
Cebit 2008
www.cebit.de

iX extra Security zum Nachschlagen:
www.heise.de/ix/extra/itsecurity.shtml

Schattenwirtschaft

Eine neue Generation von Sicherheitsrisiken

Die Berichte der Sicherheitsexperten zeigen nicht nur, dass die Zahl der Hackerangriffe weiter steigt, sondern auch, dass die Kriminellen sich der neuen Techniken und Kommunikationsanwendungen wie Voice over IP und Instant Messenger sowie der mobilen Verbreitungswege bedienen. Dahinter steht eine florierende kriminelle Schattenwirtschaft.

In den letzten neun Monaten gab es immer wieder Berichte über Sicherheitsbedrohungen, die sich von denen vorheriger Jahre vollkommen unterscheiden. Dabei lässt sich ein Trend ausmachen: Hinter den Angriffen steht ein sich ausweitendes, offensichtlich profitables Gewerbe. Sein Geschäftsfeld sind sorgsam ausgearbeitete Angriffe auf Verbraucher, Unternehmen und öffentliche Einrichtungen.

Hacker bedienen sich so schnell der neuen Technologien und Kommunikationsplattformen, dass bisher die Industrie mit ihren Gegenmaßnahmen immer einen Schritt hinterher zu sein scheint. Die klassische Firewall, die bis auf die gängigen Ports für die Standardskripts alle anderen verschließt, hat laut Experten schon längst ausgedient. Auch eine umfangreiche Schutzlösung im Stile von Unified Threat Management (UTM) könne nicht länger als „Wunderwaffe“ betrachtet werden, betonen die Fachleute.

Die in Unternehmen häufig eingesetzten Kommunikationsanwendungen wie Instant Messaging (IM) oder VoIP bedürften zusätzlichen Schutzes, den klassische Sicherheits- und Antivirenlösungen nicht immer bieten können, meinen Antivirenspezialisten etlicher Hersteller. Rootkits beispielsweise bergen ein enormes Gefahrenpotenzial. Es handelt sich dabei um kleine Programme, die Hacker einsetzen können, um Schadprogramme auf Kernel-Ebene in Rechnern zu verstecken. Die Angreifer nutzen häufig bereits bekannte Lücken in Betriebssystemen aus, die vom Unternehmen nicht ernst genommen werden.

Eine neue Dimension hat die Ausnutzung der Schwachstelle Mensch mit dem Angriff der „Zhelatin-/Storm-Worm-Gang“ – benannt nach dem von ihr verbreiteten Trojaner – erreicht. Diese Gruppe war für einen Angriff verantwortlich, der als „Storm Worm“ begann. Die Verbreitung dieses Wurms, der zum ersten Mal 2007 auftrat, begann mit E-Mails, die vorgaben, Informationen zu gefährlichen Stürmen zu enthalten, die Ende Januar in Europa wüten sollten. Nutzer, die darauf hereinfielen, wurden auf eine Website mit bösartigem

Code geleitet, der Windows-PCs in Spam-Bots verwandelte.

Im Laufe der Zeit nahmen E-Mails, die Links zum Storm Worm enthielten, diverse Formen an, von Warnungen vor angeblichen Raketenangriffen bis hin zu Berichten über Völkermord. Im Gegensatz zum typischen Blog-Spam, den die meisten kennen, schleicht sich dieser Wurm in die Blogspot-Konten von Usern ein und erstellt neue Blog-Beiträge mit Links zum Trojaner selbst. Mehrere Millionen Computer waren weltweit infiziert und Teil dieses riesigen Botnets, bis es vor ein paar Monaten in kleinere Einheiten aufgeteilt wurde.

Das Bankwesen ist auch weiterhin das primäre Ziel für Phishing-Angriffe. In den technisch immer komplexeren Trojanern implementieren Betrüger neue Angriffsverfahren, darunter Inhaltsfilter, die die Onlinebanking-Aktivitäten der Nutzer überwachen. Derartige Erkennungsverfahren machen es für Betrüger einfacher und effektiver, mithilfe verschiedener Methoden an mehr Kontoinformationen zu gelangen.

Mit Lottery Scam tauchte im Herbst eine weitere Methode des Identitätsdiebstahls auf. Hier geht es um vermeintliche Gewinne in Lotterien oder anderen Glücksspielen. Die gutgläubigen Opfer werden mit Gewinnen gelockt und auf Webseiten gelenkt, die entweder Schadcode enthalten und verteilen oder direkt nach vertraulichen persönlichen Informationen fragen. Laut einer statistischen Erhebung des United States Postal Inspection Service beziffert sich der Schaden, der durch Lottery Scams entsteht, bereits auf 120 Millionen US-Dollar im Jahr.

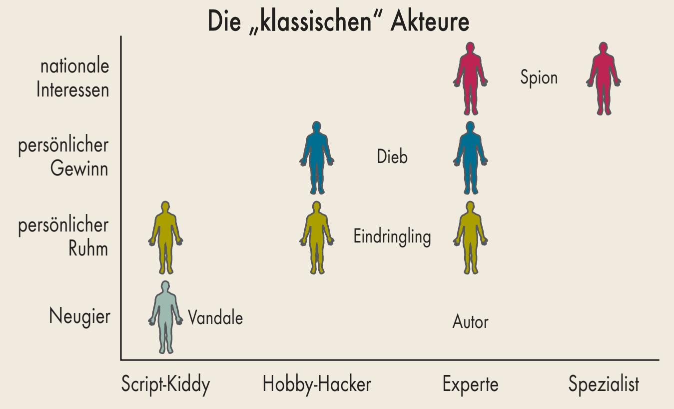
Liebesgrüße aus Nigeria

Eine besondere Rolle spielt in diesem Zusammenhang – wieder einmal – die sogenannte Nigeria-Connection. Die organisierten Gruppierungen aus Nigeria sind für die Mehrzahl der Angriffe verantwortlich. Aus diesem Grund hat die dortige Regierung nun eine Kommission eingerichtet, die mithilfe der Industrie und ausländischer Regierungen den Schaden eindämmen soll. Die Economic and Financial Crimes Commission (EFCC) berichtet, dass zumeist junge arbeitslose PC-Freaks angeheuert werden, um Lottery Scamming aus Internetcafés zu betreiben.

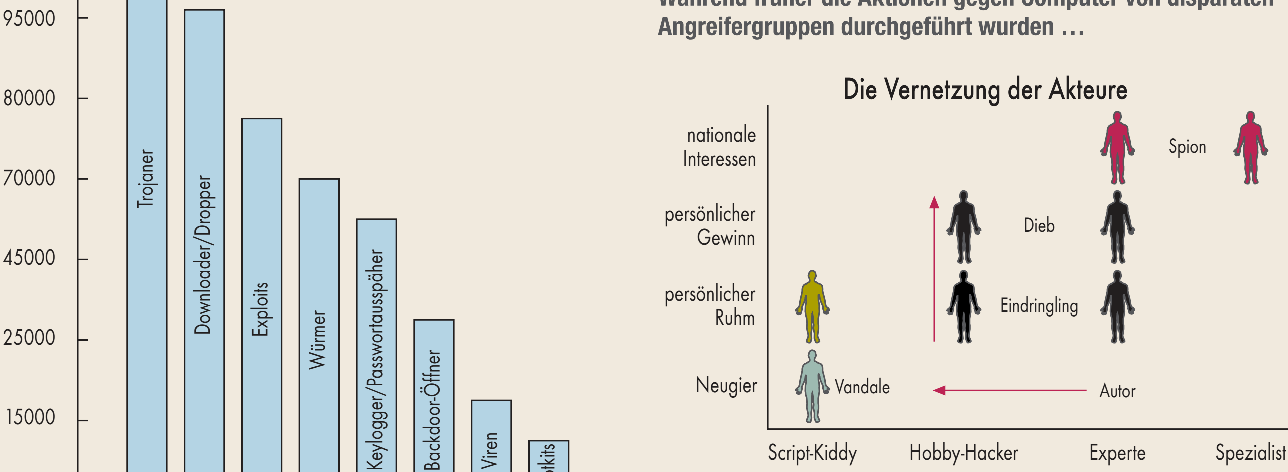
Neben der Stärkung der Abteilung für raffinierte Sicherheitsverstöße ist auch die „Mobile-Malware-Industrie“ in den vergangenen Monaten aktiver geworden. „Personalisierter“ SMS-Spam, Lotterien und Trojaner, die sich als Utility-Programme tarnen, sind Beispiele für die sich schnell entwickelnden, auf mobile Endgeräte zugeschnittenen Bedrohungen. Immer komplexere „mobile“ Trojaner und Spyware sind Auftragsarbeiten kommerzieller Organisationen, die solide Profite machen und den Ausbau dieser Schattenwirtschaft weiter vorantreiben.

Spammer waren einen Schritt voraus, als sie Bilder anstelle von Text einsetzten, um eine Hash-Filterung und einen String-Abgleich zu umgehen. Spammer nutzten auch durch Malware infizierte Computer (beispielsweise Storm-Worm-Botnets), um ihre unerwünschten Nachrichten zu versenden und eine Netzwerk-/Absender-Reputationsfilterung zu überwinden. Und als Excel, RTF, PDF und RAR archivierter Spam ist einfach nur eine Anti-Anti-Spam-Methode der nächsten Generation, die Spammer einsetzen, um einer Erkennung zu entgehen. Dieses Katz-und-Maus-Spiel ist mit der Entwicklung von Anti-Antivirentechniken vergleichbar, die Malware-Programmierer einsetzen. Als Viren mithilfe heuristischer Methoden entdeckt wurden, verlegten sich deren Programmierer auf Polymorphie, um eine Erkennung zu erschweren.

Trotz der Einführung neuer Betriebssysteme (wie Windows Vista), neuer Dienste (Inhalte für mobile Endgeräte) und Geräte (iPhone) nutzen Cyber-Kriminelle



Während früher die Aktionen gegen Computer von disparaten Angreifergruppen durchgeführt wurden …



Trojaner vorn: Microsofts Security Intelligence Report verzeichnete für das erste Halbjahr 2007 die Anzahl von Varianten pro Schädlingskategorie (Abb. 1).

… sind diese heute zunehmend vernetzt (Abb. 2 und 3).



GESUNDES WACHSTUM DURCH WEITERENTWICKLUNG

PRAXISNAHE IT-LÖSUNGEN FÜR DEN MITTELSTAND



Wir begrüßen Sie recht herzlich an einem unserer Partner-Stände bei **Intel** und **Supermicro**.

Bitte vereinbaren Sie vorab einen Termin mit unserem CPI Team unter **Tel. 0 89/96 24 41-0** oder per E-mail unter **cebit@cpigmbh.de**.

Wir freuen uns auf Ihren Besuch.



www.cpigmbh.de

weiterhin ihre altbewährten Methoden für Angriffe auf Internetnutzer. Darüber hinaus zeigt sich eine auffällige Rückkehr zu „den Ursprüngen“: Computer sind immer häufiger das Ziel von DDoS-Angriffen (Distributed Denial of Service) und Attacken, die Sicherheitslücken von Browsern ausnutzen, um dadurch in das System einzudringen. Der einzige Unterschied zwischen der Gegenwart und den vergangenen Jahren ist wahrscheinlich die Tatsache, dass E-Mail nicht mehr das primäre Medium zur Verbreitung von Viren ist. Stattdessen gehören nun Instant-Messaging-Dienste zu den hauptsächlichen Übertragungsmedien. Ein weiterer Unterschied besteht darin, dass es seit Kurzem einen explosiven Anstieg von Trojanern gibt, die auf die Nutzer von Onlinespielen zugeschnitten sind.

Selbst lernen macht schlau

Prinzipiell intelligenter werden die Bedrohungen jedoch nicht. Doch die Bedrohung der IT-Sicherheit hat sich zu einem eigenen Wirtschaftszweig entwickelt, und das verschärft das Problem.

Die am häufigsten eingesetzte Abwehrmethode mithilfe von Signaturen kann auf neue Gefahren nur mit einer bestimmten Verzögerung reagieren. Signaturen erscheinen immer etwas später als Reaktion auf einen Virus. Doch durch schnelle Netze und geschickten Code ist es möglich, innerhalb kürzester Zeit Millionen von PCs zu verseuchen. Darum propagieren einige Hersteller mittlerweile sogenannte „proaktive“ Methoden zur Entdeckung von Viren. Diese Verfahren erfordern keine Veröffentlichung von Signaturen, denn sie analysieren nicht nur den Code des zu überprüfenden Objekts, sondern auch das Verhalten von Anwendungen. Dann wird auf Basis eines Regelwerks entschieden, ob die untersuchte Software als gefährlich einzustufen ist oder nicht. Das erlaubt auch die Entdeckung noch unbekannter Schadprogramme.

Gelegentlich passiert schädlicher Code netzwerkbasierte AV-Scanner oder signaturbasierte Prüfungen, weil er als gutartig interpretiert wurde. Erst die genaue Untersuchung und eine Analyse der kombinierten Operationen sind in der Lage zu erkennen, ob aktive Inhalte tatsächlich bösartigen Code transportieren. Bereits bekannte Verhaltensmuster von Malware lassen sich in Caches speichern; wenn ein ähnliches Muster noch einmal auftreten sollte, wird diese Active Content List (ACL) abgefragt und der Schadcode entsprechend aussortiert. Besonders hervorzuheben ist die Integritätskontrolle von Anwendungen und der System-Registry. Im letzteren Fall kontrolliert der Blocker die Veränderung der Registry-Schlüssel und gestattet es, Zugangsregeln für verschiedene Anwendungen aufzustellen. Dadurch können gefährliche Veränderungen nach der Erkennung rückgängig gemacht werden. Auf diese Weise lässt sich das System nach schädlichen Aktionen unbekannter Programme sogar wiederherstellen und in den Zustand vor dem Angriff zurückversetzen.

Was die Schutzmaßnahmen im Unternehmen angeht, zeigt sich ein Wandel weg von der Perimetersicherheit hin zu einer informationszentrierten Sicherheitsarchitektur. Verantwortlich dafür sind nicht zuletzt die regulativen Bestimmungen. Im Hinblick auf die rapide zunehmende Nutzung der sogenannten Social Networks und ihren dynamisch aufgebauten Inhalten muss im nächsten Schritt der Schutz von Instant Messaging, Web 2.0 und Onlinespielen, aber auch von virtuellen Maschinen verbessert werden. (sf/JS)

Eddy Willems ist Direktor Presse und Information von EICAR (European Expert Group for IT Security).

MARKTÜBERSICHT ANTIVIRENLÖSUNGEN

Die Übersicht erhebt keine Anspruch auf Vollständigkeit.

Anbieter	Produkt	Web
Aladdin	eSafe	www.aladdin.de
Alwil	Avast	www.avast.com
Atelion	Virus Control (Norman DDS)	www.atelion.de
Authentium	Command AV	www.authentium.com
Avira	AntiVir Server	www.avira.de
Computer Associates	Antivirus, Threat Manager R8.1	www.ca.com.de
Doctor Web	Dr. Web	www.drweb-online.com
Eset	NOD32	www.eset.de
Frisk	F-Prot	www.f-prot.com
F-Secure	Anti-Virus	www.f-secure.de
G Data	AntiVirus	www.gdata.de
Grisoft	AVG Anti-Virus	www.grisoft.de
Group Technologies	iQ.Suite	www.group-technologies.com/de
Ikarus Software	Ikarus	www.ikarus.at
Intradus	Netcleanse	www.netcleanse.com
IronPort	E-Mail Gateway	www.ironport.de
ISS	Proventia-VPS	www.iss.net/emea/germany
Kaspersky	Open Space Security	www.kaspersky.de
Landesk	Antivirus	www.landesk.de
McAfee	Secure Internet Gateway, Virusscan	www.mcafee.de
Microsoft	Live One Care, Forefront	www.microsoft.com/germany
Microworld	eScan	www.microworld.de
Norman DDS	Virus Control	www.norman.de
Panda Software	Enterprise Secure	www.panda-software.de
Quick Heal	AntiVirus Plus 2008	www.quickheal.co.in
Retarus	AntiVirus Multiscan	www.retarus.de
Rising	Rising AV	www.rising-eu.com
Softwin	BitDefender	www.bitdefender.de
Sophos	Anti-Virus	www.sophos.de
Steganos	Internet Security	www.steganos.de
Symantec	AntiVirus Corporate Edition	www.symantec.de
Trend Micro	VirusWall	www.trendmicro.de
Virusblokada	VBA32	www.vba32.de

C2C schlägt B2B

Bots am Verhalten erkennen

Der Handel mit gestohlenen persönlichen Daten ist wohl derzeit das lukrativste Geschäft für Kriminelle im Online-Umfeld. Bot-Netze, Zusammenschlüsse infizierter Computer, ferngesteuert für den Datenklau oder andere kriminelle Aktivitäten einsetzbar, verzeichnen eine alarmierende Zuwachsrate. Eine der effizientesten Schutzmaßnahmen stellt das Behaviour Blocking dar, das auf der Analyse des Verhaltens von Anwendungen beruht.

Mit den sich kontinuierlich verbessernden Nutzungsmöglichkeiten des Internet nimmt auch die Motivation für kriminelle Angriffe zu. Sie werden zunehmend gezielter und haben zumeist den Datendiebstahl im Visier. Die Verbrecher müssen heutzutage nicht einmal mehr die Malware selbst programmieren, sondern kaufen im Internet ein und bedienen sich sogenannter Bot-Netze oder trojanischer Pferde, um die totale Kontrolle über fremde Computer zu erlangen.

Für den kriminellen Handel mit gestohlenen Daten oder mit Werkzeugen, die einen Identitätsdiebstahl ermöglichen, hat sich längst ein florierender Markt entwickelt. Dieses neue sogenannte Criminal-2-Criminal-Geschäftsmodell (C2C) fußt im Wesentlichen auf zwei Grundlagen: der Entwicklung von Malware oder Bot-Netzen, die an Kriminelle weiterveräußert werden, und dem Verkauf über Malware gewonnener, gestohlener Daten, aus denen die kriminellen Käufer Profit schlagen wollen.

Im Gegensatz zu den in der Vergangenheit gängigen Virenattacken basiert die Mehrzahl heutiger Cybercrime-Angriffe auf dem Web. Gut entwickelte und unsichtbar auftretende Exploits nutzen die Schwachstellen bestehender Sicherheitssysteme (etwa von Antivirenlösungen oder URL-Filter) und infiltrieren somit Computer oder ganze Netze mit Installationen, die versteckt im Hintergrund ablaufen. In den meisten Fällen nimmt der Anwender zu spät oder gar nicht wahr, dass ein Angriff stattgefunden hat. Dabei arbeiten diese Attacken nach einer ziemlich simplen Logik: Je länger der bösartige Code unentdeckt bleibt, desto mehr potenzielle Angriffsziele kann er erreichen, und desto mehr Profit verspricht er.

Zombies des 21. Jahrhunderts

Der Begriff „Bot“ leitet sich von „Robot“ ab, einem Wort, das dem tschechischen Ausdruck für Arbeit, „robota“, entstammt. Im technischen Umfeld wird darunter meist ein Programm verstanden, das ohne menschlichen Eingriff Aktionen ausführt. Einer der bekanntesten klassischen Bots ist der IRC-Bot (Internet Relay Chat) Eggdrop, der seit 1993 häufig für die Automatisierung von IRC-Funktionen eingesetzt wird. Mittlerweile versteht man unter Bots Fernsteuerprogramme, über die ein Angreifer zuvor kompromittierte Systeme zentral steuern kann. Der Zusammenschluss dieser Programme mündet in ein Bot-Netz.

Die Kontrolle über die Netze erreichen die Angreifer durch das Einschleusen trojanischer Pferde, die den Computer infizieren und dann auf Anweisungen warten, ohne auf dem infizierten Rechner Schaden anzurichten. Aktuell sind acht von zehn Schädlingen Trojaner. Hier lässt sich ein neuer Trend erkennen: Die Trojaner kommen immer öfter in Begleitung. Sobald sie sich auf dem Rechner eingenistet haben, laden sie weiteren Schadcode nach. Einen auf diese Weise gestaffelten Angriff nennt man Staged Downloader. Die Bot-Netze werden meist für Spam-Verbreitung, DDoS-Attacken (Distributed Denial of Service) oder zum gezielten Ausspionieren von Daten verwendet. Bot-Netze können aus vielen Tausenden von Rechnern bestehen, deren Bandbreitensumme die der meisten herkömmlichen Internetzugänge übertrifft.

Im Juni 2007 wurden zum Beispiel mithilfe des Trojaners MPack Toolkit über 500 000 Rechner befallen. Die Ausbeute des Bots bestand in Kundeninformationen wie Benutzername, Kennwort, Kreditkartennummer oder PIN. Sobald der Anwender eine Onlinebanking-Site aufrief, wurde der Bot aktiv und ermittelte die vertraulichen Informationen. Sogar abhängig von der Art der Inhalte (etwa bestimmte Finanzinstitutionen) reagierte der Bot entsprechend oder blieb inaktiv. Die illegal erworbenen Daten wurden anschließend über eine SSL-Verbindung übermittelt – auch Hacker sind heute sicherheitsbewusst.

Ein solches Netz aus „hörigen“ Privatrechnern ermöglicht ganz neue Formen der Internetkriminalität. Die verdeckt arbeitenden Trojaner nehmen nach dem Befall eines Rechners verdeckt Kontakt mit ihrem „Dienstherren“ auf und melden sich arbeitsbereit. Der Missbrauch des PCs kann dann ganz ungestört ablaufen, während der ahnungslose Nutzer an seinem Computer arbeitet. Die Kriminellen, die sich mit dem Aufbau solcher Netze befassen, nennen sich selbst „Herder“, also Hirten. Die gekaperten Rechner werden „Drohnen“ oder auch „Zombies“ genannt. Je mehr Drohnen ein solches Netz umfasst, desto effektiver können die Angriffe sein, die später davon ausgehen. Deshalb arbeitet jeder Zombie-Rechner nach seiner Versklavung zunächst daran, weitere Rechner in die Arme seines Hirten zu treiben. Ganz wie in den Schreckenszenarien mancher Horrorfilme: Der Angriff eines Zombies erzeugt weitere Untote.

Zahl und Größe der Bot-Netze haben massiv zugenommen. Dazu trägt die Tatsache bei, dass immer mehr Nutzer über einen Breitband-Internetanschluss verfügen und viele Computer rund um die Uhr ans Internet angeschlossen sind. Begünstigt wird diese Entwicklung auch durch die immer billigeren Internet-Flatrates, denn im Gegensatz zu analogen Internetverbindungen fällt bei DSL-Anschlüssen kaum auf, ob der Computer ungewünschte Dinge tut, weil die Verbindungsgeschwindigkeit dadurch nicht merklich sinkt. Durch Bot-Netze ist ein Rechner nicht mehr lediglich Opfer, sondern gleichzeitig auch Täter, er erhält Befehle und führt diese aus.

Ein kürzlich erschienenes Positionspapier der ENISA (European Network Information and Security Agency) beschreibt das aktuelle Ausmaß der Bot-Net-Seuche. Weltweit

sind derzeit zwischen 1000 und 2000 Bot-Netzen aktiv. Im Durchschnitt besteht jedes dieser Netze aus ungefähr 20 000 infizierten Computern. Die kleinsten Netze umfassen rund zehn und die größten nicht weniger als 300 000 Rechner. Um die 50 000 infizierte Zombie-PCs kommen täglich hinzu. Und insgesamt sind täglich nicht weniger als fünf bis sechs Millionen ferngelenkte Computer aktiv.

Bots über Mobilgeräte

Die ENISA warnt auch vor neuen Verbreitungsformen der Bots. Das Web reicht den Hackern nicht mehr aus, und es werden neue Plattformen genutzt. Neuerdings verbreiten sich Bots auch immer häufiger über Instant Messenger (ICQ, MSN, AIM und andere). Als Nächstes stehen Handys und andere mobile Endgeräte auf dem Programm. In Zukunft dürften sich kleinere, jedoch hoch spezialisierte Bots durchsetzen. Beispielsweise könnten Angreifer Nutzern suggerieren, dass sie E-Mails oder Weblinks von Freunden oder Kollegen zugeschickt bekommen. Die so gewonnenen Informationen werden zielgerichtet zum Passwortklau oder gar zur Betriebsspionage ausgenutzt.

Kriminelle bauen ihre modernen Bot-Netze nun häufig über Peer-to-Peer-Verbindungen auf. In diesem Fall gibt es keinen zentralen Server mehr, über den die Bots kontrolliert und gemanagt werden. Ein gezieltes Aufspüren und vor allem das Lahmlegen ganzer Bot-Netze wird also zunehmend schwieriger. Und nicht zuletzt verändern sich Bot-Netze durch Zufallsroutinen permanent selbst. Aus der Entfernung werden ihre Funktionen automatisch ständig weiterentwickelt – sie mutieren quasi am laufenden Band. Und dabei verändern sie die Spuren, die sie auf ihren Wirtsrechnern hinterlassen, und sind dadurch immer schwieriger aufzuspüren.

Zombies zur Miete

Wie bereits erwähnt, ist der heutige Internetkriminelle nicht mehr notwendigerweise ein versierter Programmierer. Viren, trojanische Pferde und auch Bot-Netze lassen sich heutzutage einfach und bequem anmieten. Und wie im ganz normalen Leben gibt es Qualitätsunterschiede: Je besser ein Bot getarnt ist und je mehr Rechner infiziert sind, desto wertvoller ist ein Netz. Pro gekidnapptem Rechner und Tag verlangen Bot-Manager ungefähr ein bis vier Euro. Besonders leistungsfähige Rechner können bis zu 70 Euro kosten. Speziell chinesische Täter bieten Dumpingpreise: Für weniger als einen Euro pro Tag lässt sich ein Bot-Rechner anmieten und für die eigenen Zwecke einsetzen.

Bot-Netze sind ein internationales Problem, und die ENISA fordert deshalb nicht nur ihre EU-Mitgliedstaaten zu mehr Zusammenarbeit auf, sondern ist der Meinung, es müsse ein internationaler Austausch und Zusammenschluss auf Behördenebene stattfinden, um die Netze effektiv aufzuspüren und die Verwalter dingfest zu machen. Ein erster Schritt dahin besteht in der Umsetzung von Awareness-Kampagnen, die auf das Phänomen aufmerksam machen. Nicht wenige Experten sehen jedoch insbesondere die Internetprovider in der Pflicht. Diese tun nach Ansicht vieler Fachleute nämlich immer noch zu wenig, um ihre Netze gegen Schädlinge und Eindringlinge zu schützen. Wie in den USA sollten sich auch deutsche Provider über die Entdeckung neuer Bot-Netze besser austauschen und übergreifende schwarze Listen erstellen.

Auch in puncto Prävention und Benutzersensibilisierung hinken die Provider immer noch hinterher, von einigen löblichen Ausnahmen abgesehen, die ihre Kunden vor Gefahren warnen und auf mögliche Bot-Netz-Infektionen hinweisen. Dabei wird auch schon mal die DSL-Verbindung gekappt, insbesondere wenn der Provider einen Spam-Massenversand von einem bestimmten Rechner feststellt.

Behaviour Blocking als Schutzmaßnahme

Das sogenannte Behaviour Blocking analysiert das Verhalten der gestarteten Anwendung und blockiert gefährliche Aktionen. Auf diese Weise lässt sich ein effizienterer Schutz gegen trojanische Pferde, die Bots transportieren, aufbauen als mit signaturbasierten Methoden. Im Unterschied zur heuristischen Analyse, die verdächtige Handlungen im Emulationsmodus (dynamische Heuristik) untersucht, arbeiten Behaviour Blocker (Verhaltensblocker) unter realen Bedingungen. Die neue Generation von Verhaltensblockern analysiert nicht nur einzelne Aktionen, sondern auch die Abfolge von Handlungen. Das bedeutet, dass die Beurteilung der Gefahr, die von einer Anwendung ausgeht, auf einer komplexen Analyse basiert.

Moderne Verhaltensblocker sind in der Lage, ein breites Spektrum von Ereignissen im System zu analysieren und zu kontrollieren, vor allem potenziell gefährliche Aktivitäten wie alle gestarteten Prozesse oder Speicherung aller Veränderungen im Dateisystem und in der Registry. Wird eine verdächtige Aktion gestartet, erhält der Nutzer eine Warnung über dessen Gefährlichkeit. Zudem erfasst der Blocker das Eindringen des schädlichen Programmcodes in fremde Prozesse und entdeckt auch sogenannte Rootkits, also Programme, die die Arbeit des schädlichen Codes in Dateien, Ordnern und der Registry verbergen sowie gestartete Programme, Systemdienste, Treiber und Netzverbindungen verstecken.

Zwischen proaktiven Lösungen und Behaviour Blocking gibt es Unterschiede. Proaktive Ansätze untersuchen Muster und assoziieren sie mit bekannten Schadcode-Listen. Diese Lösungen untersuchen nicht das Verhalten des Inhalts, sondern den Inhalt selbst. Darum sind diese Produkte nicht in der Lage, zu verstehen, wie sich ein Browser beim Laden einer bestimmten Webseite tatsächlich verhält. Diese Art von Produkt kann die Webseite nicht als Ganzes betrachten, weil sie nur individuelle Pakete sieht. Das ist ein Grund, warum solche Lösungen nur schwer Spyware oder Phishing-Attacken erkennen können.

Der gesamte Kontext einer drohenden Ausführung eines Angriffs lässt sich tatsächlich lediglich auf der Anwendungsebene (beispielsweise im Browser) erkennen und das Verhalten sowie Auswirkungen interpretieren. Es gibt unzählige Wege, Schadcode zu verstecken – der einzige Weg, das Verhalten zu erforschen, besteht in der Analyse, während die Anwendung läuft.

Im Kampf gegen die Bot-Netze haben die Anwender selbst immer noch die stärksten Waffen in ihrer Hand. Da sich die meisten Angriffe im Internet abspielen, sind eine Firewall und ein aktuelles Antiviren-Programm ebenso ein Muss wie das Aufspielen der aktuellsten Updates auf das Betriebssystem. Vorsicht ist auch beim Öffnen von unbekannten Links geboten. Dies gilt ebenso für E-Mail-Anhänge von unbekannten Personen. (sf/JS)

Manuel Hüttl
Vorstandsmitglied der EICAR (European Expert Group for IT Security) und General Manager DACH bei Waggener Edstrom



Klare Vorteile für KMUs, Konzerne und Service Provider

Managed Security Services

Der Markt für Managed Security Services wächst beständig, jedoch gilt dieser als schwierig und kostenintensiv. Clavisters neue Security Service-Plattform beseitigt diese Probleme und ermöglicht es so Resellern, Systemhäusern, IT-Abteilungen und Service Providern effizient auf dem Outscouring-Security-Markt zu agieren.

Die Clavister Security Service-Plattform (SSP) steht für das gesamte Clavister-Produktportfolio von Security-Gateways, UTM-Appliance- sowie Management Systeme und den damit zusammenhängenden Sicherheits-Services. Diese Lösung, kombiniert mit den Clavister Lifecycle-Systemen FineTune, PinPoint, und Insight setzt einen neuen Standard für Managed Security Services, da sich einerseits die Total Cost of Ownership (TCO) auf ein Minimum reduzieren lässt und andererseits ein rascher Return of Invest (ROI) erreichen lässt: sowohl für KMUs, die ihre Security an externe Dienstleister auslagern, als auch für Konzerne, die über interne IT-Serviceabteilungen verfügen und Service Provider, die ihren Kunden wiederum Sicherheitsdienstleistungen anbieten wollen. FineTune und PinPoint werden von Clavister kostenlos angeboten, wodurch Manage Security Service Provider im Gegensatz von herkömmlichen Lösungen massiv Geld sparen können. Die Hardware-Basis in den Zentralen bilden dabei UTM-Appliance-Systeme der 4000er-oder 3000er-Systemreihen. Zur Anbindung von Niederlassungen kommt die SG10-Serie zum Einsatz. Die SG10-Serie garantiert Manage Security Service Providern eine optimale und sichere Anbindungen von kleinen Firmen oder Außenstellen. Damit werden Kompromisslösungen vermieden, die Service Provider in der Vergangenheit dazu gezwungen hatten sich zwischen Standardprodukten mit unzureichenden Funktionen oder teuren Lösungen mit unnötig vielen Features zu entscheiden. Die SG10-Serie bietet darüber hinaus noch weitere Vorteile: Beispielsweise kann eine Antivirus Scan-Engine und eine Supportfunktion für Clavisters InSight Reporting- und Logfile-Analyse-System integriert werden. Ebenso enthält die Serie eine Web Content Filtering-Funktion sowie ein Intrusion Detection und Prevention (IDP/IPS) System.

Die Lösung ermöglicht einen schnellen und kosteneffizienten Einsatz der Managed Security Services (MSS), beispielsweise in den Bereichen:

Managed VPN
Managed Wireless Network Protection
Managed Firewalling
Managed Intrusion Detection and Prevention (IDP)
Managed Antivirus Protection
Managed Content Filtering
Managed Web-Use Reporting
Managed Regulatory Compliance Reporting

Die **Clavister SSP-Plattform** zeichnet sich durch die Fähigkeit aus, sich an das Wachstum der Unternehmen anpassen zu können (Clavister xPansion Lines). Hierzu wurde die Lösung mit Feinabstimmungsmechanismen und hochgradig skalierbaren Funktionen ausgestattet, die es jedem Betreiber ermöglichen, diese an seine individuellen Leistungs- und Funktionsanforderungen nahtlos anzupassen. Die Tatsache, dass sowohl der Clavister SSP als auch das Customer Premise Security Gateway (CPE) dasselbe hoch skalierbare Betriebssystem Clavister CorePlus™ verwenden, macht jegliche Kompromisse zwischen maximalem Service, Verfügbarkeit, Funktionalität, Steuerbarkeit, TCO sowie Kapitalinvestitionen hinfällig.

Mit **Clavister FineTune** steht den Anbietern von Managed Security Services ein modernes, graphisch orientiertes Management-System (GUI) zur Verfügung, das die zentrale Verwaltung einer Vielzahl von Clavister Security-Gateways aus einer benutzerfreundlichen GUI-Umgebung heraus, ermöglicht. Über dieses Management-System ist die Remote-Verwaltung aller Clavister-Devices inklusive deren Konfiguration, Real Time-Monitoring sowie -Logging, Revisionskontrolle und Firmware Upgrades möglich und wird via 128-Bit-Verschlüsselung und Authentifizierungsmechanismen effektiv geschützt.

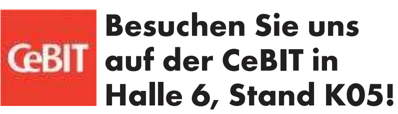
Mit **Clavister-PinPoint™** ist ein neues Tool verfügbar, mit dem Sicherheitsprozesse in Echtzeit überwacht werden können. Dieses ermöglicht Security Managern über eine intuitiv zu bedienende Oberfläche einen grafischen Überblick u.a. über Surfgewohnheiten, Resultate von Virus- oder Malware-Scans, Einbruchsversuche in das Netzwerk oder VoIP-Statistiken. Vergleichbar mit einem Flugzeug-Cockpit, können die „Piloten“ von PinPoint essenzielle Daten (Mission Critical) von weniger wichtigen (Non-Critical) unterscheiden und anzeigen lassen. Clavister ist der erste Hersteller, der eine einfach zu bedienende Applikation auf den Markt bringt, die Security-abhängige Vorfälle in Echtzeit visualisiert.

Durch **Clavister InSight** wird diese Plattform mit erweiterten Funktionen für das Logging und Monitoring von Security-Events und um umfassende Alarm- und Forensikfunktionen ergänzt. InSight bietet eine leistungsfähige „Security-Intelligenz“, die automatisch alle Event-Daten von Clavister-Systemen und anderen Multi-Vendor-Netzwerkgeräten wie Router oder Switches etc. sammelt, kontrolliert und re-



portet. InSight liefert folgende fortschrittliche Security-Intelligence-Features wie zum Beispiel: GUI (Graphical User Interface)-basierter detaillierter Event-Drilldown, User-definierbare Event- und Threat-Level-Klassifizierung, Heterogenes Real-Time-Monitoring, zusammengefasstes Reporting und viele weitere wertvolle Funktionen.

Auch wenn die Firmen noch zögern, insgesamt mehren sich die Anzeichen dafür, dass sich der MSS-Markt in einem Aufschwung befindet. Das zeigt die Umsatzentwicklung der europäischen Security-Outsourcing-Anbieter: Die Analysten von Gartner bescheinigen diesen eine durchschnittliche jährliche Wachstumsrate von 14,9 Prozent.



Tel.: +49 40 411259-0
E-Mail: info@clavister.de, www.clavister.de

CeBIT **Besuchen Sie uns auf der CeBIT in Halle 6, Stand K05!**

Clavister-Aktion zur CeBIT 2008: Sichern Sie sich Ihr kostenloses Security Gateway!
Die ersten 50 Besucher, die sich unter www.clavister.com/ix registrieren, können sich die kostenlose Clavister-P12 Softwarelizenz herunterladen und sich somit Ihr eigenes Clavister Security Gateway erstellen. Diese Version unterstützt 2 Netzwerkkarten und verfügt über einen Durchsatz von 10Mbit/s. **Viel Glück!**

Trojanersturm

Neue Formen des Datendiebstahls

Das Geschäft mit kriminell motivierten Cyber-Angriffen wächst sich zu einem ernsthaften Problem aus, das längst BKA und Dienste interessiert. Schließlich geht es um international organisierten Identitätsklau und Datendiebstahl. Phishing mit E-Mails, die auf gefälschte Webseiten verweisen, und Pharming sind dabei nur zwei Spielarten. Immer häufiger werden Daten mit trojanischen Pferden gestohlen.

Datendiebstahl ist längst nicht mehr nur die Domäne von Wirtschaftsspionen, Geheimdiensten und Terroristen. Kriminelle Banden haben den Wert von Daten erkannt. Phishing ist ein Versuch, vertrauliche Daten von Anwendern durch gezielte Täuschungsmanöver zu stehlen. Seit den ersten Betrugsversuchen dieser Art Mitte der 1990er-Jahre ist die Anzahl der Phishing-Attacken erheblich gestiegen. Die Betreiber der Sammelstelle Phishtank berichten über eine Steigerung der Anzahl von Phishing-Betrugsangriffen um 254 Prozent von Januar bis April 2007. Der Service Phishtank des kalifornischen Unternehmens OpenDNS sammelt bekannte Phishing-Webseiten in einer Datenbank, die durch die internationale Open Source Community ständig aktualisiert wird.

Angriffsziel Onlinebanking

Die größte Zielgruppe sind nach wie vor Kunden von Onlinebanken – insbesondere in Ländern, wo PIN und eine einfache TAN die einzige Barriere zwischen Dieb und Konto bilden (beispielsweise Großbritannien und USA). Wie hoch der Schaden durch Onlinebanking-Betrug ist, lässt sich nur schätzen. Deutsche Banken schweigen sich über die Schadenssummen aus. Der Bitkom geht für 2006 von 3250 Phishing-Fällen mit einem mittleren Schaden von jeweils 4000 Euro aus – zusammen also 13 Millionen Euro. Viele Fälle kommen aber gar nicht erst ans Licht der Öffentlichkeit, da die betroffenen Personen und Organisationen Rufschädigung befürchten. Diese Zahlen belegen, dass der Diebstahl von Informationen ein florierendes Geschäft ist.

Komplettdiebstahl der Identität

Schon lange nicht mehr sind die Aktivitäten auf Onlinebanking-Daten begrenzt. Manche Datenspione stehlen auf infizierten Rechnern alle Eingaben in Formulare. Davon sind dann auch Zugangsdaten zu Social-Networking-Foren, E-Mail-Postfächern, Onlineshops, Jobbörsen oder Chat-Räumen betroffen. Im einfachsten Fall verkaufen die Kriminellen die Daten unsortiert auf dem Schwarzmarkt. Die Zugangsdaten können aber auch zur Geldwäsche und zum Versand von Foren-Spam genutzt werden. Im Jahresbericht von Phishtank belegen die gefälschten Seiten von Ebay und dessen Bezahldienst Paypal mit Abstand die Spitzenplätze. Die anfänglichen Probleme mit Zeichensätzen und Sprache sind

überwunden, und dank flexibler und einfach zu bedienender Tools wie Rockphish können mehrere Phishing-Seiten auf einer Website gehostet werden.

Einen Schutz gegen Phishing bieten Spam-Filter. Sie erkennen Phishing-Mails und verhindern deren Zustellung. Der Zugang zu Phishing-Seiten kann aber auch auf anderen Wegen erfolgen: beim Chat, in Spielen, in Foren. Anti-Phishing-Toolbars in Browsern warnen vor Phishing-Seiten oder verbieten den Zugang komplett. Der Internet Explorer 7 oder Firefox 2.xx sowie viele Internet-Sicherheitslösungen enthalten sie von Hause aus. Diese Toolbars setzen einerseits auf heuristische Verfahren zur Erkennung „schlechter“ URLs. Dabei besteht jedoch immer die Gefahr eines False Positive, deshalb sind die Regelsätze recht konservativ. Viele Anbieter setzen zusätzlich auf die Kraft der Community. Wer eine gefälschte Webseite findet, meldet sie dem Response-Team des Anbieters, das sie verifiziert und gegebenenfalls in eine schwarze Liste aufnimmt. Nachteil dieses Verfahrens: Das Verifizieren der Seite dauert zu lang – ähnlich wie das Erstellen von Virensignaturen. Bei Phishtank sind das im Durchschnitt knapp zwei Tage, bei kommerziellen Anbietern wenige Stunden. In diesem Zeitfenster können die Datendiebe ungestört agieren.

Die Anwender sensibilisieren

So bleibt die Sensibilisierung des Anwenders, wie in so vielen Betrugsszenarien, das wichtigste Mittel im Kampf gegen Datenverlust. Beim Umgang mit persönlichen Daten sollten alle Internetnutzer sehr vorsichtig sein; den Benutzern muss klargemacht werden, dass bei sicherheitsrelevanten Eingaben der überprüfende Blick auf die URL zum Pflichtprogramm gehört: Links ein https:// muss sein, und den Domain-Namen von ganz rechts lesen sollte man auch immer. Das ist zwar immer noch keine 100-prozentige Garantie gegen Fake-URLs, aber man hat wenigstens die dümmsten Formen der Irreführung ausgeschlossen.

Pharming: Angriff auf DNS-Server

Pharming ist eine Technik, die Benutzer unbemerkt auf falsche Webseiten leitet, obwohl diese den korrekten Domänennamen im Browser eingegeben hatten. Basis dieser Angriffe ist die Ermittlung der IP-Adresse einer Domain. Dazu kann das DNS-System selbst angegriffen werden. Schlecht gewartete oder konfigurierte DNS-Server bieten Angreifern Möglichkeiten, den Cache der DNS-Server mit falschen Informationen zu füllen (DNS Cache Poisoning genannt) oder den DNS-Server anderweitig zu kompromittieren.

Ebenso liefern Client-Rechner Ansatzpunkte zum Aushebeln des DNS-Systems. Diese werden hauptsächlich von Trojanern genutzt. Kundige PC-Anwender können sich vor lokalen DNS-Angriffen schützen, indem sie kritische Links, etwa den zu ihrer Onlinebank, als IP-Adresse in den Favoriten speichern.

Eine weitere Technik für den Identitätsdiebstahl ist der Einsatz von Trojanern. Diese bestreiten mittlerweile die überwiegende Mehrheit der Phishing-Angriffe. Die vielfältigen Schutzmechanismen gegen Phishing und die fortschreitende Aufklärung der Nutzer zeigen Wirkung. Auch die Gegenmaßnahmen der Geldinstitute wie iTAN (indizierte TANs), mobile TAN (nach Übersendung der ausgefüllten Überweisung im Internet erhält der Nutzer von der Bank per SMS eine nur für diesen Vorgang verwendbare TAN), Token für zeitlich begrenzte TANs und HBCI (Home Banking Computer Interface) tragen dazu bei, dass die gephishten Informationen nicht mehr verwertet werden können. Die Kriminellen brauchen – zumindest in den meisten Ländern – neue Mittel, um die Daten abzugreifen. Zu diesem Zweck setzen sie unterschiedliche Arten von Crimeware ein.

Gefahr durch Keylogger

Keylogger zeichnen Tastaturaktionen auf. Sie können als Treiber realisiert sein oder Informationen an den im Betriebssystem dafür vorgesehen Schnittstellen abrufen (*WinAPI SetWindowsHook* oder *WinAPI GetKeyboardState*). Zur Tarnung integrieren sie sich in gängige Systemprozesse (*winlogon.exe, services.exe*) oder nutzen Rootkits. Oft schlagen sie nur zu, wenn bestimmte Bedingungen erfüllt sind, etwa wenn die gerade geöffnete Webseite in einer oft sehr langen Liste von Domänennamen enthalten ist oder wenn der Benutzer ein Fenster mit bestimmten Inhalten öffnet. Als Gegenmaßnahme wurden Bildschirmtastaturen entwickelt. Die Reaktion darauf sind wiederum Screenlogger. Diese schießen entweder in regelmäßigen Abständen Bilder des gesamten Bildschirminhalts (Rbot) oder erzeugen bei jedem Mausklick eine Grafik des Mausumfelds. Manchmal werden die Bildsequenzen auch gleich in eine AVI-Datei umgewandelt.

Einige Schädlinge (zum Beispiel Torpig) verändern das Aussehen des Browsers. Sie sind in der Lage, die Adresszeile mit der korrekten Anschrift darzustellen, obwohl die Inhalte von einem anderen Server kommen. Auch das Schloss, das eine verschlüsselte Verbindung symbolisiert, lässt sich simulieren.

Manche Schädlinge (etwa Bancos-Varianten oder Nurech) manipulieren die Inhalte bestimmter Webseiten und fügen entweder weitere Formularfelder oder ganze Webseiten ein. Dabei bleiben bestehende SSL-Zertifikate aktiv. Ohne die Hilfe spezieller Tools ist es nicht möglich zu erkennen, ob diese Daten gefälscht sind oder nicht. Die so gewonnenen Daten werden sowohl an die Angreifer als auch an die echten Webserver geschickt. Nach dem Datendiebstahl wird die Sitzung normal fortgesetzt, sodass bei den Opfern kein weiterer Verdacht entsteht. Erst der Blick auf die Abrechnung offenbart den Angriff.

Frühe Session Hijacker unterbrachen die Verbindung des Opfers, nachdem es seine Daten eingegeben hatte. Das weckte unmittelbar nach dem Angriff Verdacht. Seit einiger Zeit werden Sessions so übernommen, dass die Angreifersoftware zwar die Beträge und Kontoangaben zu seinen Gunsten ändert (beispielsweise mit Bancos), dem Opfer aber dessen Angaben anzeigt – bis hin zur „Korrektur“ des Kontostands. Auch hier ist der Betrug erst beim Blick auf die Kontoauszüge ersichtlich.

Angriff auf *hosts*-Datei

DNS-Spoofing nutzt, wie bereits erwähnt, häufig die lokalen Möglichkeiten, einem Domänennamen eine falsche IP-Adresse zuzuweisen. Ein Angriffspunkt, den die Malwarefamilie QHosts häufig nutzt, ist die Datei *hosts* im Verzeichnis

ONLINEQUELLEN

[1] Anti-Phishing Working Group, www.antiphishing.org

[2] Phishtank Annual Report, Okt. 2007, www.Phishtank.com/blog/2007/10/09/’ Phishtank-annual-report/

[3] Keylogger. Funktionen und Erkennungsmethoden. Teil 2, www.viruslist.com/de/analysis?pubid=200883538

[4] Finjan Malicious Page of the Month, July 2007, www.finjan.com

[5] Ihr Ebay-Passwort: 3, 2, 1 – meins, www.heise.de/security/news/meldung/54272

[6] BITKOM. Zahl der Phishing-Opfer steigt in Deutschland weiter, www.bitkom.org/de/presse/8477_47739.aspx

[7] APACS. Fraud the Facts 2007, www.apacs.org.uk/resources_publications/documents/FraudtheFacts2007.pdf



C:\windows\system32\drivers\etcetera, in der Host-Namen IP-Adressen zugewiesen sind. Wenn dies gelingt, bedarf es keiner weiteren Versuche, die gefundene IP-Adresse zu verifizieren. Eine andere Möglichkeit bieten die Einträge für die DNS-Server. Sind diese so manipuliert, dass sich die DNS-Anfragen an einen vom Angreifer kontrollierten Server richten, gibt es für die meisten Seiten korrekte Ergebnisse – aber für einige eben nicht.

Redirector wiederum lenken den Datenfluss so um, dass ein Man-in-the-Middle-Angriff möglich wird, durch einen lokalen Proxy oder einen Proxy-Server, der unter der Kontrolle des Angreifers steht. Darüber lässt sich die gesamte Netzkommunikation des Opfers belauschen – E-Mails, Chats, besuchte Webseiten, Formulardaten, Datei-Downloads und so weiter.

Sniffer fangen den Datenstrom in einem Netzwerk ab. Mittels ARP-Spoofing funktioniert das auch in nicht geswitchten Netzwerken. Spy-Trojaner schließlich durchsuchen den gesamten PC nach verwertbaren Informationen. Das können E-Mail-Adressen sein oder Dateien mit bestimmten Inhalten oder eines bestimmten Dateityps. Diese Daten werden gepackt und an den Angreifer gesendet. Sehr beliebt sind auch auf dem System gespeicherte Login-Informationen, Registrierungsschlüssel und Passwörter (oder deren Hashes).

UTM als Grundschutz

Für jede Einzelne dieser Bedrohungen sind spezielle Lösungen erforderlich, die sich an der jeweiligen Situation orientieren müssen. Unified Threat Management (UTM) bietet einen soliden Grundschutz. Solche Systeme integrieren unterschiedliche Sicherheitstechniken wie Firewall, Antivirus, Intrusion Detection oder Intrusion Prevention in ein Gerät. Anhänger des „Best of Breed“-Konzepts kaufen die jeweils besten Einzelkomponenten und nehmen die umständlichere Konfiguration in Kauf.

Viele Webseiten erzeugen ihre Inhalte aus Datenbanken. Interaktive Funktionen werden über Eingaben in Formularfelder gesteuert. Doch ungefilterte Eingaben können die Inhalte der Datenbank auslesen und/oder manipulieren. SQL Injection ist eine der häufigsten Angriffsarten auf Datenbanken. Aber auch per Cross-Site Scripting und Pufferüberlauf lassen sich Datenbankinformationen stehlen. Durch zielgerichtete Phishing- oder Crimeware-Angriffe können die Zugangsdaten des Datenbankadministrators gestohlen werden. Hier sind die Entwickler der Webseiten oder -anwendungen gefordert, jedes Eingabefeld auf Stimmigkeit zu prüfen.

Wie auch beim Schutz vor Computerschädlingen können technische Lösungen nur einen Teil der Angriffe abwehren.

Immer misstrauisch bleiben

Gegen Datenklau und Identitätsdiebstahl gibt es zwar sowohl speziell entwickelte Softwarelösungen als auch allgemeine, umfassende Ansätze. Man sollte sich jedoch nicht in falscher Sicherheit wähnen und keinen hundertprozentigen Schutz erwarten. Darum ist und bleibt die Umsicht und Vorsicht besonders wichtig. Das Internet ist ein Ort, an dem kriminelle Betrüger aktiv sind. Und deshalb ist ein richtiges Maß an Misstrauen das effektivste Mittel.

(sf/JS)

Manuel Hüttl ist Vorstandsmitglied der European Expert Group for IT Security (EICAR).
Ralf Benzmüller ist Leiter der SecurityLabs von G DATA.

Einbruchsicherung

Intrusion-Detection- und Intrusion-Prevention-Systeme

Erfolgreiche Angriffe lassen sich nie hundertprozentig ausschließen, auch wenn präventiv wirkende Tools wie Firewalls und Antiviren-Scanner vorhanden sind. Darum ist es wichtig, die Folgen einer Infektion oder eines Hackerangriffs so gering wie möglich zu halten.

Es gibt viele Wege, auf denen Schadcode auf einzelne Computersysteme oder in ein ganzes Netz gelangen kann. Selbst wenn die Verantwortlichen ihre präventiv tätigen Sicherheitssysteme wie die Firewall und den Antiviren-Scanner richtig konfiguriert und aktualisiert haben und sich die meisten Benutzer durch Schulungen der Gefahr durch mobile Datenträger bewusst sind – eine einzige unbedachte Tat genügt. Systeme für Intrusion Detection und Intrusion Prevention können durch schnelles Aufdecken des Angriffs die Folgeschäden verringern respektive eine Attacke verhindern.

Der Begriff der „Intrusion“ schließt dabei jede nicht autorisierte Handlung ein. Insbesondere gilt dies natürlich, wenn die Handlung die Funktion des Systems beeinträchtigt. Zu möglichen Intrusions gehört neben dem klassischen Angriff eines Hackers von außen der Missbrauch des Systems durch einen regulären Benutzer.

Intrusion-Detection-Lösungen nehmen im Wesentlichen drei Teilaufgaben wahr. In der Disziplin Angriffs-/Einbruchserkennung (klassische Intrusion Detection) versucht die Software beispielsweise, den Einbruch in einen Webserver zu entdecken. Die Missbrauchserkennung (Misuse Detection) untersucht, ob Benutzer oder Programme sich gemäß den Sicherheitsregeln verhalten oder ob sie beispielsweise Zugriff auf verbotene Internetdienste oder Ordner im Dateisystem erlangen wollen. Über die Erkennung von Anomalien (Anomaly Detection) würde es dem System unter anderem auffallen, wenn plötzlich ein Netzwerkprotokoll benutzt wird, das vorher nicht im Einsatz war.

Seit gut fünf Jahren bieten die Sicherheitshersteller zusätzlich Intrusion-Prevention-Lösungen. Ausgehend von der Intrusion Detection versucht eine solche Software, direkt den erkannten Angriff zu stoppen. Um dies bewerkstelligen zu können, muss ein IPS die gerade stattfindende Attacke erkennen und vor ihrer Vollendung unterbinden. Im Gegensatz zu einem klassischen IDS, das lediglich reaktiv Alarmmeldungen generiert, muss ein solches System proaktiv arbeiten.

Klassifizierung der Intrusion Detection

Im Allgemeinen lassen sich IDS in zwei Gruppen einteilen: in hostbasierte Systeme (Host Intrusion Detection System – HIDS) und in netzwerkbasierte Systeme (Network Intrusion Detection System – NIDS). HIDS sind Systeme, die nur einen Rechner überwachen und vom Betriebssystem, den Anwendungen oder der Netzwerkverbindung erzeugte Daten auswerten. Eine solche Lösung muss also vor allem vom Betriebssystem unterstützt werden, und das stellt auch gleichzeitig den größten Nachteil eines HIDS dar: Ist das jeweilige Betriebssystem und damit der ganze Rechner selbst kompromittiert, kann der Angreifer auch das IDS manipulieren. Um Eindringlinge zu entdecken, liest ein HIDS typischerweise die Log-Dateien des Betriebssystems sowie der Serversoftware (Mail-, Web-, Datenbankserver et cetera).

Ein HIDS kann Angriffe erkennen, die innerhalb von vernetzten Systemen nicht einfach aufzudecken sind. Hostbasierte Systeme haben zudem Zugang zu detaillierten Daten über Systemprozesse, Ressourcenverwendung und Geräteaktivität, die netzbasierten Sensoren fehlen. In einigen Fällen kann die Analyse dieser Daten die einzigen Indizien für einen Angriff liefern. Dies ist beispielsweise bei einem Einbruch durch einen Insider der Fall. Wenn der Angreifer in demselben lokalen Netzwerk sitzt wie das Zielsystem, wird der Verkehr wahrscheinlich nicht über einen Sensor eines NIDS laufen.

Ein NIDS bezieht seine Informationen aus der Analyse von Netzwerkpaketen, die es üblicherweise über einen Netzwerk-Sniffer, den sogenannten Sensor, erhält. Netzbasierte IDS sind vor allem geeignet, Angriffe und Einbrüche von außen zu erkennen. Sofern ein interner Täter Rechner über Netzgrenzen hinaus angreift, kann dies ein NIDS ebenso aufdecken. Das System könnte beispielsweise überprüfen, ob zwischen dem Webserver und dem Datenbankserver tatsächlich ausschließlich SQL-Requests in Richtung Datenbankserver laufen. Die üblichen Angriffsmuster von Denial-of-Service-Attacken (DoS) oder Port-Scans lassen sich ebenso zuverlässig aufdecken. Auch Zugriffe auf typische Ports durch Rootkits, trojanische Pferde oder Backdoors sind leichte Beute für ein NIDS.

Unterschiedliche Erkennungstechniken

Ein weiteres Unterscheidungsmerkmal von Intrusion-Detection-Systemen stellt die eingesetzte Technik beim Aufspüren von Unregelmäßigkeiten dar. Allerdings sind die Übergänge häufig fließend. Die Erkennung kann beispielsweise auf der Grundlage von Signaturen geschehen. Die dabei notwendigen Muster (Signaturen) liegen in einer Datenbank ähnlich einer Virensignatur und werden mit den zu überprüfenden Daten – beispielsweise beim Transport übers Netz – verglichen. Unbekannte Muster lassen sich auf diese Weise allerdings nicht als Angriff identifizieren. Aus diesem Grund gibt es eine Anomalieerkennung. Das IDS lernt also erst mit der Zeit, welche Datenströme und Aktionen im Netzwerk „normal“ sind und schlägt Alarm, wenn ein Vorgang davon abweicht. Viele IDS nutzen beide Methoden.

Die Konfiguration des Intrusion-Detection- und -Prevention-Systems stellt Verantwortliche vor eine große Herausforderung. Sie müssen sehr sorgsam vorgehen, um möglichst wenige Falschmeldungen zu generieren. Grundsätzlich gibt es zwei Möglichkeiten einer Falschmeldung: Ein falsch-positiver Alarm durch das System bezeichnet eine Meldung, die eigentlich keinen Alarm auslösen sollte – also der klassische Fehlalarm. Einzelne Meldungen sind zunächst recht harmlos, kommen sie aber häufig vor und sind nicht abschaltbar, führt dies über kurz oder lang zu Desinteresse – und es werden auch echte Alarmmeldungen übersehen. Während diese Fehlalarme in reinen IDS-Umgebungen zunächst nur lästig sind, hat in einer Intrusion-

Prevention-Umgebung die Blockierreaktion des IPS auf einen Fehlalarm schlimme Folgen, da die Kommunikation unschuldiger Personen blockiert wird.

Falsch-negativ benennt einen fehlenden Alarm durch das System, wenn eigentlich einer hätte ausgelöst werden müssen, da ein Einbruch stattgefunden hat. Dies ist besonders kritisch, da es einem Angreifer nur einmal gelingen muss, eine Schwachstelle auszunutzen, um Zugang zu einem System zu bekommen. Falschmeldungen können Verantwortliche nur durch sorgfältige Konfiguration, Kenntnis der überwachten Netze und Systeme sowie aufmerksame Analyse der auflaufenden Meldungen vermeiden. Sie sollten vor allem nach Änderungen in der Infrastruktur oder nach der Neuinstallation von Servern beziehungsweise Diensten die Konfiguration des IDS und IPS überprüfen und gegebenenfalls anpassen.

Netzwerkbasierte Intrusion Prevention

Unter dem Begriff NIPS sind eine Vielzahl unterschiedlicher Ansätze und Produkte vereint. Dazu gehören klassische IDS-Produkte, die bei einem im Netz erkannten Angriff automatisch versuchen, diesen zu blockieren, aber genauso Webfilter, die Angriffe auf Anwendungsebene durch eine Analyse aller Webseiten, Links, Formulare und Benutzereingaben im HTTP-Verkehr zu verhindern versuchen. Netzwerkbasierte IPS nutzen unter anderem die folgenden Techniken:

– Beenden einer TCP-Session durch Reset-Pakete,
– Blockade weiterer Kommunikation von der Quelladresse des Angriffs durch Einfügen entsprechender (temporärer) Regeln in Firewall-Systemen sowie
– Verwerfen der Pakete eines erkannten Angriffs im System, das den Datenverkehr als Proxy transportiert.

Wie bei allen automatischen Reaktionen auf Angriffsversuche halten auch diese Lösungen einige Herausforderungen bereit. Viele Angriffe beziehen nur wenige Pakete ein, oft passt der eigentliche Exploit in ein einziges Datenpaket. Die eigentliche Schadsoftware beziehungsweise die Kommunikation mit einem Einbrecher nutzt dann eine andere Verbindung, sodass das IPS diese häufig nicht als dem Angriff zugehörig klassifiziert. Das Beenden der Angriffsverbindung durch ein Reset-Paket hätte also keine Schutzwirkung.

Das Problem dynamisch erstellter Firewall-Regeln ist, dass sie nicht schnell genug auf den Firewalls umgesetzt werden, da die Angriffe oft nur Bruchteile von Sekunden dauern. Bei der Auslastung von typischen Firewalls kann diese schnelle Umsetzung schwierig sein. Außerdem muss sichergestellt werden, dass ein Angreifer dieses Feature nicht zu einem Denial of Service benutzt, indem er Pakete, die eine Angriffssignatur enthalten, mit der Absender-IP eines gewünschten Kommunikationspartners versendet. Dieser wäre dann ungerechtfertigterweise via Firewall-Regel blockiert. Das Problem ist technisch lösbar: Wenn das IPS vor dem Eingriff in die Kommunikation sämtliche TCP-Verbindungen überwachen würde, könnte es anhand der ausgetauschten Sequenznummern erkennen, ob die Quelladresse eines Angriffs gefälscht ist. Diese Methode funktioniert allerdings nicht bei statusloser Kommunikation mit UDP.

Zusätzlich zu den klassischen Reverse-Proxies gibt es IPS-Produkte, die nicht nur die HTTP-Ebene betrachten, sondern die semantische Integrität jedes einzelnen Eingabefeldes in jeder Benutzermaske auf seine individuellen Beschränkungen hin prüfen. Attacken wie SQL-Injection und viele andere Angriffe auf Webanwendungen lassen sich damit blockieren, bevor sie überhaupt zum Webserver gelangen.

Hostbasierte Intrusion Prevention

Hostbasierte Intrusion-Prevention-Systeme laufen üblicherweise als Agenten auf Servern und Desktops und kontrollieren alle Zugriffe auf Ressourcen von Anwendungen. Unerlaubte Zugriffe wie Schreibbefehle auf Systembibliotheken oder Registry-Einträge können sie direkt verhindern. Die Entscheidungsgrundlage, ob ein Zugriff erlaubt oder verboten ist, bildet eine Richtlinie, die entweder der Hersteller für gängige Anwendungen mitliefert oder die in einem Lernmodus (halb)automatisiert erstellt werden kann. Da eine zu umfangreiche und komplexe Richtlinie in der Praxis sehr schwer zu warten ist und häufig zu Problemen führt, verwendet man oft nur sehr einfache. Mit wenigen Regeln lässt sich beispielsweise verhindern, dass ein Netzwerkdienst (wie Web- oder Mailserver) weitere externe Programme startet. Während ein klassisches HIDS nur Alarm schlägt, kann das hostbasierte IPS direkt auf dem System unerwünschte Zugriffe auf Systemressourcen und damit unter Umständen einen Schaden verhindern.

Wilhelm Dolle
ist Sicherheitsberater bei der HiSolutions AG in Berlin.

In iX extra 4/2008:

Storage – Energieeffiziente Server- und Storage-Systeme

Alle Hersteller propagieren inzwischen ihre „Green IT“ – was sich aber häufig nur in bunten Anklebezetteln erschöpft. Wer es ernst meint mit Einsparungen beim Stromverbrauch der heutigen Server- und Storage-Systeme, muss sich auf die Suche nach den Gründen für die Explosion der Energiekosten machen. Modische Einsparungen bei CPU oder Lüftern sind nur begrenzt hilfreich, auch insgesamt kann im Rahmen der Produktion der IT-Komponenten nur ein bescheidener Beitrag zur Energieeinsparung geleistet werden. Interessanter wird es allerdings, wenn man die gesamte Infrastruktur des Rechenzentrums mit einbezieht.

Erscheinungstermin:
20. März 2008

DIE WEITEREN IX EXTRAS

Ausgabe	Thema	Erscheinungstermin
05/08 Networking	VoIP-PSTN-Gateways	17.4.08
06/08 Mobility	Applikationen auf dem USB-Stick; Notebooks klein und leicht	15.5.08
07/08 IT-Security	Information Loss Prevention & Device Management	19.6.08